Operator's Manual (OM)
Tripwire 1.0.0.2 for HP-UX 10.10
31 January 1997

Introduction: Tripwire is an integrity checker. It allows you to know if certain files you have told Tripwire to check have been changed or altered. If you check all important files on your system that do not change frequently, you will significantly improve your system security.

To run via icon: Simply double click on the Tripwire icon. You will be asked whether you want to replace the database (/h/COE/Comp/TRIP/bin/databases/TRIP.database) and configuration files with their backups. If you choose 'y', and xterm will appear for you to replace the files. Next, you will be asked whether you wish to run Tripwire in interactive mode. This mode allows you to update your database file for any valid changes to the files being checked. See below (Updating the Database File) for more information. When run via icon, Tripwire will send the results of the run to standard output, i.e. to the screen. This output is not saved, so if you close the xterm before you are done, you will have to run Tripwire again.

To run via crontab: Tripwire will run automatically every week early Sunday morning, if this setting was enabled at installation, either manually or by running /h/COE/Comp/TRIP/Scripts/TRIP.tripwire_weekly_config. In this case, the output will be mailed to sysadmin, and will be saved in /h/COE/Comp/TRIP/data/tripwire.results. If you only run Tripwire via crontab, you shuld ensure that the database and configuration files are secure. It is highly recommended that you run Tripwire via icon (and replace the database and configuration files) regularly, because an intruder could have found and amended the files to cover up changes to your system.

Updating the Database File: There may be valid changes to the files and/or directories Tripwire checks. In this case, it is necessary to update the database file to reflect the changes. There are two ways of doing this:
1) Run Tripwire via the Tripwire icon, and chose interactive mode. This will allow incremental updates to the database file. You will be prompted whether or not to update the entry in the form, "---> Update entry? [YN(y)ng?]". The choices 'y' and 'n' are conventional yes and no, while 'Y' and 'N' tell tripwire yes or no for all updates. The choices 'h' and '?' give help and descriptions of the various inode fields. You should use caution in choosing the 'Y' option, as that may update the database file for changes that you haven't considered yet. It is strongly recommended that you refrain from using the 'Y' choice. When you are done updating the database file, DO NOT forget to update your backup copies of the database file.

In case of Intrusion: If you know or suspect that an intruder has gained access to your system: At the minimum, replace the database and configuration files with the ones you have on your backup media. It is also recommended that you reinstall Tripwire from the original distribution, as the actual Tripwire binaries may have become corrupted. If you you reinstall Tripwire, DO NOT follow the original installation instructions and create a new database file. Instead, just copy your backups into the appropriate place, and run Tripwire normally. This should tell you of all the changes to the files you have told Tripwire to monitor.